

El futuro de la identidad digital

9 expertos opinan
sobre las nuevas tecnologías financieras y la verificación de la identidad digital

icar

Las tecnologías financieras han facilitado la operativa bancaria a muchísimas personas.

La banca es cada día más digital. Operaciones tan habituales como consultar el saldo bancario, realizar una transferencia o solicitar divisa extranjera ya no requieren desplazarse hasta un cajero u oficina.

Para el usuario, un hecho como ahorrarse ir hasta la oficina y hacer cola para una simple transacción es ya un increíble valor añadido, en una época en la que el tiempo es uno de los activos más valiosos.

Para las **empresas y entidades financieras** este cambio de paradigma se ha traducido en la necesidad de **adaptarse a los canales digitales** con nuevos modelos de negocio, tecnologías disruptivas y una inversión constante en seguridad digital.

Pero los avances conllevan dudas que no siempre son fáciles de resolver. Conceptos como la tecnología **blockchain**, las tecnologías **biométricas** y su papel en la **seguridad digital**, la **verificación del usuario** o el cumplimiento con **la normativa** a menudo plantean más preguntas que respuestas.

Aunque el ánimo de este ebook no es resolver todos los interrogantes, sí que hemos querido arrojar un poco de luz sobre los principales conceptos alrededor de las tecnologías financieras y la identidad digital del usuario, a través de la visión de diez expertos.

¿Qué encontrarás en este ebook?

- Las experiencias y opiniones de diferentes expertos del sector financiero, tecnológico, legal y de empresa.
- Los cinco conceptos que más impacto tienen actualmente en la verificación de la identidad digital.
- Los datos más relevantes sobre el futuro de la identidad digital, a partir de estudios seleccionados.
- Una visión global sobre la evolución de las tecnologías financieras.



Contenidos

1.

La conexión entre el yo físico y el yo digital

La necesidad de conectar el yo físico con el yo digital es cada vez más evidente, tanto para mejorar la experiencia del usuario como para aumentar la seguridad de las relaciones digitales. Pero, ¿qué es la identidad digital? El hecho es que probablemente no tenemos una sola, sino varias. Así, el reto no es unificar las identidades digitales para identificar mejor al usuario, sino conectar todo el contexto digital que representa al usuario en internet.

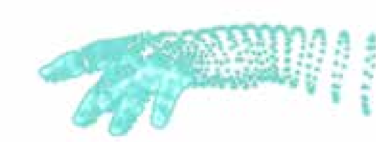
El siguiente paso es entender qué supone realmente esta identidad. En este sentido, las empresas pueden ayudar al usuario a comprender mejor la dimensión real del mundo digital, un mundo que ya cuenta con una entidad propia, que va más allá de ser un simple reflejo del mundo offline.

Y en este contexto, las empresas juegan un papel esencial, no solo en la implementación de nuevas tecnologías, sino en generar confianza en el usuario a través de la comunicación y la información.

El mundo online ya no es un simple reflejo del mundo offline.


ICAR
Qué nos ha enseñado el #MWC17 sobre el futuro de la identidad digital
17 de marzo de 2017

Tenemos que entender y conectar todo el contexto digital que representa a las personas en Internet.

75% de consumidores

posee algún otro dispositivo además de smartphone, ordenador o portátil.


Más de la mitad de usuarios del mundo

utiliza un smartphone.

+ de 1 de cada 5 personas

compraron online en los últimos 30 días.

Connected devices, consumers and the future of payments. Payments & VISA report 2017

Xavier Codó
CEO de ICAR



« Hoy en día prácticamente **cualquier persona tiene una identidad digital**, formada no solo por sus datos personales y financieros, sino por sus relaciones con las empresas y su comportamiento en la red.

Cualquier transacción, cualquier acción, deja un rastro que se suma a nuestra identidad digital y ayuda a definirla con más precisión. Por otra parte, lógicamente, una de las principales preocupaciones respecto a esta identidad es la seguridad, tanto para el usuario, que pueda sentir que sus datos están expuestos, como para la empresa, que debe identificar que su cliente es quien dice ser para evitar el fraude y la suplantación de identidad.

> La tecnología nos permite responder cada vez mejor a los retos de seguridad, sin renunciar a una experiencia sin fisuras, rápida y cómoda.

En un proceso de onboarding, por ejemplo, **la seguridad se establece durante el proceso de registro y autenticación**. Este proceso debe verificar la identidad de la persona, que esta realmente existe y es quien dice ser; comprobar sus datos personales y contrastarlos con bases de datos de terceros, de forma totalmente segura y que no los exponga; y autenticar los documentos, validando las diferentes medidas de seguridad que incorpore.

Por suerte, la tecnología nos permite responder cada vez mejor a los retos de seguridad, sin renunciar a una experiencia sin fisuras, rápida y cómoda.

Porque, si de una cosa estamos seguros, es de que el futuro de los modelos de negocio pasa por su capacidad de adaptarse a los nuevos consumidores digitales, y esto implica una actualización constante de la tecnología y de los procesos digitales. »

Fernando García-Quismondo
Tecnología Corporativa de Grupo Santander



« Día a día nos encontramos ante una nueva realidad en la que los actos de nuestro yo físico tienen **una trazabilidad cada vez mayor** como resultado del rastro que deja nuestro yo digital.

El uso de la biometría es y será fundamental a la hora de establecer el nexo de unión entre nuestra dimensión física y la digital.

Esto es algo que sin duda nos aportará enormes beneficios, pero también grandes riesgos que debemos afrontar cuanto antes. Como usuarios, empezamos a entender que nuestros patrones de consumo, nuestra geolocalización, nuestro entorno social..., son datos con un elevado valor para cualquier empresa, y por ello queremos que esas empresas que los gestionan nos garanticen **privacidad, control y confianza,** una confianza que es esencial en esta nueva dimensión digital en la que ya nos encontramos, donde la identidad y los datos son el nuevo oro.

Por eso hay algunos factores clave para hacer frente a esos desafíos que nos plantea el mundo digital: El uso de la biometría es y será fundamental a la hora de establecer ese nexo de unión entre nuestra dimensión física y la digital. Y, del mismo modo, el uso de **blockchain y smart contracts** permitirá aportar al usuario un control de esa información que le representa.

Combinando ambos elementos, un usuario podría dar permiso de acceso únicamente a aquellos datos que desee compartir en el ledger de blockchain, y además podría autorizar dicho acceso empleando su biometría, que de este modo se convierte en el proxy principal entre su yo físico y su yo digital. »



Josep Grau
CaixaBank Innovació

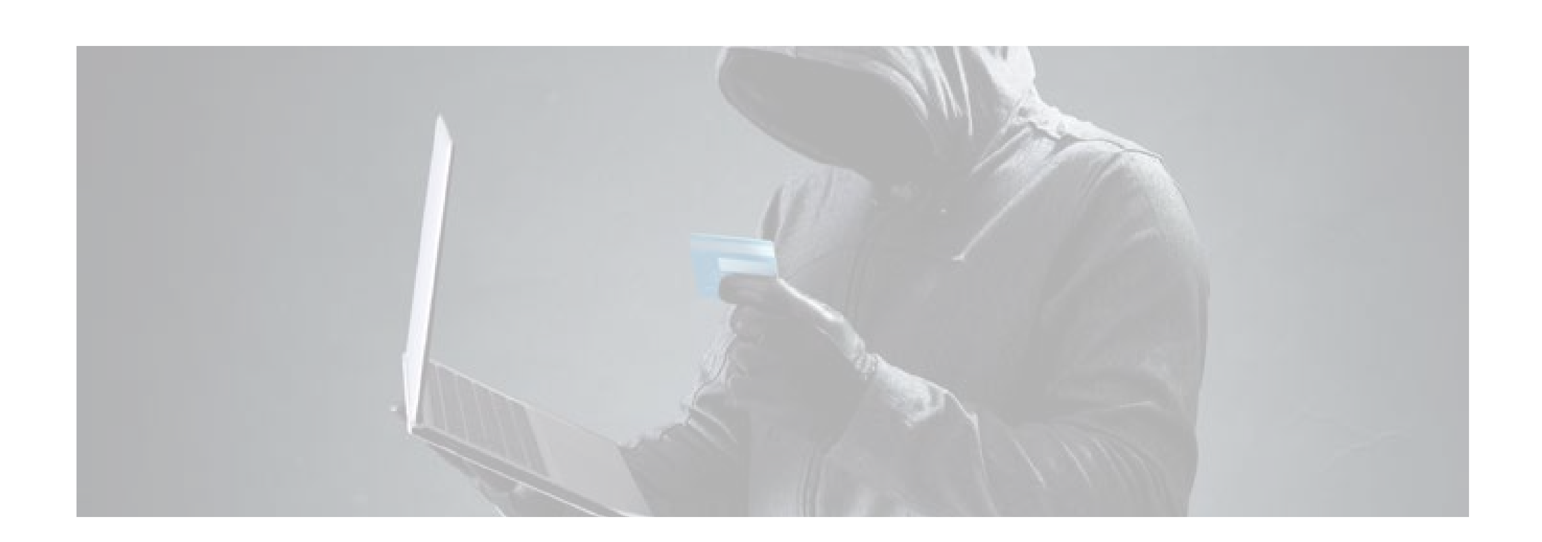


« De nada sirve tener una identidad digital si no puede ser utilizada para actividades del día a día. Si bien es cierto que actualmente **la mayoría de personas dispone de una identidad digital**, esta va más allá de la que aparece en redes sociales tanto lúdicas como profesionales.

> Existe el riesgo de la creación de múltiples identidades para una misma persona o la suplantación de identidad por parte de un tercero.

Pero, más allá de los beneficios que pueda comportar la posesión de una identidad digital, existe el riesgo de la creación de múltiples identidades para una misma persona o la suplantación de identidad por parte de un tercero.

Así, en un mundo solo digital donde existe un mapeo con el mundo físico, las consecuencias de una suplantación pueden llegar a ser graves en el caso de solicitar préstamos o realizar compras por internet. »



2.

Las tecnologías biométricas



La identificación por biometría no es un concepto de este siglo, ni tan siquiera del pasado. En la China del s. XIV ya se imprimían en tinta y papel las palmas de las manos y los pies de los niños para identificarlos. Y en la Babilonia del 500 a.C. se utilizaban tablas de barro con huellas dactilares impresas en transacciones comerciales.

La idea de que cada persona es única no es nada nuevo. Pero no ha sido hasta este siglo que la biometría ha alcanzado un uso más extendido, gracias en gran parte a la democratización de la tecnología.



Los procesos basados en sistemas biométricos son más cómodos, rápidos y eficientes para el usuario.

95% - 99%

de fiabilidad en reconocimiento facial por biometría.

ICAR, datos sobre implementación de sistemas biométricos

Otro factor a favor de esta tecnología es que los datos demuestran que la autenticación y la verificación por biometría son mucho más seguras que los sistemas tradicionales, especialmente con las mejoras que se están introduciendo constantemente a nivel tecnológico.



ICAR
Biometría: Cuando nuestro cuerpo nos identifica
24 de marzo de 2017

La autenticación y verificación por biometría son mucho más seguras que los sistemas tradicionales que incluyen un proceso manual.

de 600 M$ a casi 2.000 M$

pasarán los pagos móviles biométricos del 2016 al 2017.

Juniper Resarch

casi 160 M

de dispositivos estarán habilitados con biometría para la actividad bancaria en el 2020.

Biometría para servicios financieros, Google Intelligence

Javier Mira
CEO de FacePhi



« Hoy en día, la biometría ha experimentado un crecimiento imparable, lo que ha permitido que esté presente en diversos sectores, especialmente en el financiero. Gracias a que proporciona una alta seguridad y conveniencia al usuario, está en proceso de expansión hacia otros sectores tan dispares como el sanitario y la automoción.

En la actualidad, el 75% de las compras e interacciones con nuestro banco se realizan en el entorno online, y por tanto la gestión de nuestra identidad digital es un tema capital. Es aquí donde la biometría jugará un papel fundamental.

Las biometrías más usadas en la actualidad son la facial, huella y voz, pero aún falta mucho camino por recorrer. **Se estima que en 2020 se llegue al 100% de bases instaladas de la biometría en los dispositivos móviles;** además se prevé que las tarjetas de crédito tengan sensores biométricos. Con la identidad biométrica no será necesario disponer de identidad física, y será posible hacer cualquier transacción desde cualquier parte sin necesidad de contraseñas, provocando que muchos de los problemas como el spoofing y man-in-the-middle pasen a la historia.

Por otra parte, uno de los problemas que surgen en la actualidad y afectan al futuro de la biometría es la tecnofobia. **El desconocimiento de las nuevas tecnologías provoca inseguridad** frente a ellas. Para poder implementar la biometría al 100% es necesario educar a la sociedad de manera que puedan considerar la biometría como un proceso natural. Y para ello, es necesario invertir tanto en tecnología como en enseñar a los usuarios a utilizarla. Por eso, consideramos que **la experiencia de usuario es indispensable**. En este sentido, FacePhi ha invertido mucho en conocer las necesidades del usuario final, y podemos decir que el alto porcentaje de adopción de la tecnología de reconocimiento facial de FacePhi por parte de los clientes de entidades financieras se debe principalmente a la experiencia de usuario.

A nuestro modo de ver, el reconocimiento facial unido a la Inteligencia Artificial (AI) será clave en el futuro de la biometría, teniendo en cuenta que es la manera natural de identificación entre los seres humanos. Y gracias a la facilidad de capturar una cara con la cámara desde cualquier dispositivo de la manera menos intrusiva, nos permitirá una adopción masiva de la tecnología. »

Eric Gracia
Abogado en Derecho.com



« La biometría como método identificativo está de moda, especialmente en el ámbito de la banca, donde permite **reducir el uso de papel, prevenir el fraude y facilitar la contratación de productos a distancia.** No obstante, esto plantea importantes riesgos que han sido tenidos en cuenta por la normativa de privacidad más actual. Así, los datos biométricos aparecen específicamente definidos en el nuevo Reglamento General de Protección de Datos europeo (aplicable a partir del 25 de mayo de 2018) como "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos". De hecho, la norma considera que **los datos biométricos son una categoría especial de datos personales** y reconoce a los Estados miembros la capacidad de introducir condiciones o límites adicionales para su tratamiento.

Por tanto, la regla general es que el tratamiento de datos biométricos está prohibido a menos que se haya obtenido el consentimiento explícito de la persona interesada para ello.

Esta protección legal reforzada está plenamente justificada, pues ¿Qué pasaría si alguien se apoderase de la plantilla biométrica con la información en claro obtenida a partir de nuestra huella dactilar o nuestra imagen facial, datos biométricos con los cuales nos identificamos para, por ejemplo, autorizar operaciones con el banco? Cuando la seguridad de una contraseña se ve comprometida podemos cambiarla, pero nuestra huella o nuestra cara no (al menos no de forma fácil).

Por ello, deben aplicarse en estos casos técnicas de biometría cancelable, que permitan generar un nuevo dato biométrico para el mismo individuo en caso de ver comprometida su seguridad. Además, es recomendable que al capturar la muestra biométrica nos aseguremos de que está "viva". Sin olvidar que la identificación biométrica suele recomendarse como complemento de otros medios de autenticación, como por ejemplo una contraseña, si bien **los constantes avances en este campo acabarán por ofrecernos identificaciones biométricas cómodas de usar y suficientemente robustas por sí solas.** »

Xavier Codó
CEO de ICAR



« El novelista Frederick Buechner ya dijo que "me veo forzado a concluir que, hasta un extremo alarmante, yo soy mi rostro". Esto puede ser más cierto de lo que pensamos, ya que nuestra cara y nuestros datos biométricos nos identifican inequívocamente más que cualquier otro elemento.

Los datos biométricos son prácticamente imposibles de falsificar. Y dado que **nuestro rostro está indiscutiblemente ligado a nuestra identidad**, las tecnologías que permiten relacionar uno con otra se están perfilando como las más fiables para identificar al usuario en los procesos de verificación de la identidad.

Pero, **¿es el reconocimiento facial por biometría realmente fiable?** Los datos indican que sí, sin duda. Las soluciones actuales dan un porcentaje de fiabilidad entre el 95% y el 99%. Es cierto que no es el 100% deseado (todavía), pero en cualquier caso es un porcentaje mucho más elevado que el reconocimiento efectuado por personas y de forma manual, que incluso realizado por agentes entrenados y con fotografías de calidad puede alcanzar un margen de error del 14%.

Las soluciones actuales dan un porcentaje de fiabilidad entre el 95% y el 99%.

Además, las tecnologías biométricas aplicadas a la verificación de la identidad digital se combinan con otros procesos de identificación, como por ejemplo el cruce de datos con bases de datos de terceros, la geolocalización o el SNA (Análisis de Redes Sociales), con lo que se dobla o triplica el factor de autenticación.

En mi opinión, **las tecnologías biométricas son extremadamente seguras y válidas como sistema de identificación del usuario**, además de rápidas y cómodas. Las reticencias y dudas a su uso probablemente tienen más que ver con el desconocimiento y la falta de información que con su fiabilidad en si. »

3.

La tecnología blockchain

Una de las tecnologías más disruptivas que han surgido como consecuencia de la transformación digital de empresas y entidades financieras es la blockchain. De forma muy simplificada, consiste en una base de datos distribuida que incluye una lista de registros ordenados en constante crecimiento y actualización. Estos registros se almacenan de forma segura y privada, y constituyen un inmenso historial de todas las transacciones, inversiones, operaciones, contratos..., y cualquier operación financiera que tenga un rastro digital.

La tecnología blockchain está redefiniendo no solo cómo opera el sector, sino toda la economía financiera global.

Así, es seguro que la tecnología blockchain supondrá un cambio sustancial en la forma de entender la banca y las finanzas personales. Pero este cambio parece que será progresivo y gradual, no tan repentino como otros cambios a los que la tecnología nos tiene acostumbrados, ya que necesita superar unas barreras que no se desmontan fácilmente.

ICAR
Cómo afecta la tecnología blockchain al sector financiero
24 de marzo de 2017

La esencia de la tecnología blockchain es la compartición de información. Esto requiere, entre otras cosas, un cambio de mentalidad en las empresas y entidades financieras.

95%
de los usuarios

espera que su banco cuente con las últimas tecnologías para proteger la seguridad de su información financiera.

Mastercard Safe and Security Survey 2015

77%
de los usuarios

espera adoptar tecnología blockchain como parte de un sistema de producción o proceso para el 2020.

Global Fintech Report 2017. PwC

Fernando García-Quismondo
Tecnología Corporativa de Grupo Santander



« **El uso de blockchain y smart contracts podría romper con las barreras** y retos que suponía la colaboración entre compañías, abaratando al mismo tiempo sus costes operativos, ya que podrán ahorrarse procesos de verificación internos, que podrán venir establecidos desde entidades ajenas a nosotros a través de esta tecnología.

Además, dentro del ámbito europeo debemos tener en cuenta la aplicación de la nueva GDPR (General Data Protection Regulation), en la que **el cliente tendrá mucho más control sobre sus datos**, sobre quién tiene acceso a ellos y sobre la portabilidad de dichos datos entre compañías.

El uso de blockchain y smart contracts podría romper con las barreras a la colaboración entre companías.

En este contexto, iniciativas como el ecosistema multisectorial basado en blockchain recientemente creado en España, y del que el Banco Santander es uno de sus socios fundadores, podrían suponer un cambio que facilitará el camino hacia la creación de nuevos modelos de negocio.

Esta red no solo es inédita en el mundo (hasta ahora no existía ninguna red multisectorial con un espacio de trabajo digital conjunto), sino que podría permitir entre otras cosas el lanzamiento de un sistema de identificación digital segura que **facilitará el intercambio de datos** cumpliendo con todos los requisitos regulatorios, lo que daría al cliente la máxima garantía en cuanto a seguridad, privacidad y control sobre su propia información. »

Josep M. Garcia

Socio y fundador de IoT Infinitum Projects



« Estamos ante un cambio de paradigma en el uso de la información por parte de los clientes, las empresas y las administraciones públicas. La razón es que hasta hoy la información estaba centralizada, exclusiva de cada agente del sistema, alterable y protegida a ojos de terceros para que se considerase segura. Este paradigma obliga a que siempre existan participantes que verifiquen y acrediten que la información es cierta.

La tecnología blockchain propone **un cambio donde las transacciones se pueden hacer en un mundo abierto, transparente, descentralizado y dejando una traza que lo hace inmutable y, por lo tanto, seguro.**

Eso implica que los modelos de negocio deben comprender, al igual que lo han hecho las criptomonedas, que no es necesario un Estado respaldando una moneda para que esta tenga valor y credibilidad.

Pero esta tecnología se enfrenta a una visión de los directivos y responsables de la Administración que perciben las posibilidades de blockchain como una amenaza, ya que disuelve de pronto muchas de las ventajas competitivas que definen las estructuras de diversos mercados.

Un registrador de la propiedad, mercantil o un notario serán absolutamente innecesarios (por poner solo algunos ejemplos). Para las empresas, todos los sistemas de pagos y cobros, información comercial o legal…, estarán a disposición de cualquiera que pueda comprobarlos.

Por ello la gran duda que se pone encima de la mesa es cómo se gobernará el sistema y qué limitaciones se impondrán, y qué plataformas y aplicaciones interactuarán con el conjunto del ecosistema. Estas decisiones determinarán la potencia que el blockchain pondrá en nuestras manos y qué condiciones se van a abrir para crear modelos de valor completamente nuevos, y que destruirán muchos de los tradicionales.

La tecnología blockchain genera demasiadas dudas para que los grandes actores económicos se planteen realmente la extensión de su uso. Solo las grandes compañías del sector de internet pueden a día de hoy ser las grandes beneficiadas de su introducción, al virtualizar servicios y productos.

Cuando todavía estamos asistiendo al éxito incipiente de las criptomonedas, ya empezamos a observar las inquietudes que estas generan en los Estados y las empresas. De momento la amenaza es pequeña, aunque real, y está claro que **el potencial de cambio es enorme.** »

Josep Grau
CaixaBank Innovació



« El uso de las Distributed Ledger Technologies (DLT), como sería el caso de blockchain, podría ayudar al sector financiero a demostrar la identidad del cliente, con detalles como la fuente de los fondos, los intereses comerciales o la historia, así como también supervisar el progreso en el camino.

Cada banco e institución financiera tiene que realizar el proceso de KYC (Know Your Customer) individualmente, y cargar la información y los documentos validados en un registro central que almacenaría los datos digitalizados etiquetados con un número de identificación único para cada cliente.

Un registro único basado en blockchain **eliminaría la duplicidad de esfuerzos en la realización de controles KYC**. El ledger (nombre que recibe la base donde se almacenan tales datos) podría permitir que las actualizaciones cifradas de los detalles del cliente se distribuyan a todos los bancos casi en tiempo real.

Otros beneficios de crear una DLT para la gestión de la identidad serían la reducción de los costes y el aumento de la seguridad.

Este modelo potencial de uso de una identidad digital proporciona beneficios significativos para KYC:

- Experiencia de usuario mejorada, dado que solo tendría que presentar la documentación una vez.
- Mayor seguridad (menos oportunidad de robo de identidad).
- Menos transacciones que se marcan como falsos positivos.

Otros beneficios que puede aportar la creación de una DLT para la gestión de la identidad serían la reducción de los costes operacionales para los bancos, por no tener que comprobar cada cliente (si ya han sido verificados y se les ha dado una identidad digital), un **aumento de la seguridad gracias a la distribución casi en tiempo real de la documentación actualizada de KYC** y una mayor transparencia para los reguladores.

A su debido tiempo, una identidad digital podría ser utilizada en muchas industrias, no solo para transacciones financieras. »

Reynold G. Pereira

Owner of LegalTech English

(A Legal & Business Consulting Firm)



« La tecnología blockchain nos ofrece la posibilidad de cruzar los límites jurisdiccionales, ya que los nodos en un blockchain se pueden encontrar en cualquier parte del mundo. Esto podría crear una serie de cuestiones jurisdiccionales complejas que requerirían un estudio cuidadoso en relación con las relaciones contractuales pertinentes.

Los principios de contrato y título difieren entre las jurisdicciones, y por lo tanto la identificación de la ley aplicable es esencial. En una transacción bancaria tradicional, por ejemplo, si el banco es culpable, independientemente del mecanismo de transacción o de la ubicación, puede ser demandado y la jurisdicción aplicable será muy probablemente regida contractualmente. Sin embargo, **en un ambiente descentralizado puede ser difícil identificar el conjunto apropiado de reglas a aplicar.**

En su nivel más simple, cada transacción podría caer bajo la jurisdicción o jurisdicciones de la ubicación de cada nodo en la red. Claramente, esto podría resultar en un blockchain que necesita ser compatible con un gran número de regímenes legales y reguladores. En el caso de que se realice una transacción fraudulenta o errónea, señalar su ubicación dentro de un blockchain podría ser un reto.

Por lo tanto, **la inclusión de una cláusula exclusiva de ley aplicable y jurisdicción es esencial**, y debe garantizar que el cliente tenga seguridad jurídica en cuanto a la ley que se aplicará para determinar los derechos y obligaciones de las partes en el acuerdo y qué tribunales resolverán cualquier disputa. »

Se debe garantizar que el cliente tenga seguridad jurídica en cuanto a la ley que se aplicará para determinar los derechos y obligaciones de las partes.

4.

La experiencia del usuario



El reto de una excelente experiencia de usuario es el equilibrio entre usabilidad y seguridad: si una tecnología tiene una UX óptima pero un bajo nivel de seguridad, se incrementan las pérdidas por fraude online; si tiene una UX pobre pero elevadas barreras de seguridad, pierde clientes, y por lo tanto también beneficio. En ambos casos se pierde la confianza del usuario.

Ante este escenario, ¿Cuál de los dos factores es realmente importante? La clave del éxito es conseguir que la experiencia de usuario y la seguridad sean sinónimos. Para ello, es necesario ser proactivos, conocer a nuestro usuario y transformar sus requerimientos en una experiencia agradable, sin olvidar su creciente preocupación por la seguridad de sus datos.

> La experiencia debe ser cada vez más multicanal, especialmente en móvil y social media.

 **ICAR**
Seguridad y UX, tendencias clave en el eFintech Show
29 de marzo de 2017

> Es necesario simplificar los procesos y operaciones. No se trata simplemente de traspasar los procesos offline a online, tienen que repensarse desde una perspectiva 100% digital.

86% de los consumidores

están dispuestos a invertir tiempo y dinero en adoptar nuevos métodos de pago a cambio de la promesa de una mayor seguridad.

Mastercard Safe and Security Survey 2015

83% de los consumidores

dice que utilizar dispositivos conectados para pagar le ahorrará tiempo y/o reducirá su frustración a la hora de realizar un pago.

Connected devices, consumers and the future of payments. Payments & VISA report 2017

77% de consumidores conectados

ve a su entidad financiera como el intermediario o sistema de pago más fiable, por encima de Google, Apple, Microsoft o Facebook.

Connected devices, consumers and the future of payments. Payments & VISA report 2017

Fernando García-Quismondo
Tecnología Corporativa de Grupo Santander



« En mi opinión la experiencia de usuario es uno de los desafíos más grandes al que nos enfrentamos no solo las empresas, sino también los propios usuarios. Si bien es cierto que las empresas y la regulación deben buscar que los mecanismos que apliquen sean de uso sencillo, los usuarios deben también tener en cuenta que en el entorno digital es posible ser víctima del cibercrimen, y que a menudo los controles que marca la regulación, o las presuntas "barreras tecnológicas" que en su opinión anteponen las empresas, no tienen como finalidad perjudicar su uso, sino todo lo contrario: hacerlo más seguro, transparente y trazable.

Las empresas deben aplicar modelos más flexibles, sencillos y personalizados, que permitan hacer que la seguridad se convierta en una experiencia cómoda para los usuarios.

Encontrar **ese equilibrio entre seguridad, cumplimiento y experiencia** es el reto al que se enfrentan las empresas y los usuarios.

Los primeros probablemente deban aplicar modelos más flexibles, sencillos y personalizados, que permitan hacer que la seguridad se convierta en una experiencia cómoda para los usuarios; y los segundos tener en cuenta el importante rol que juegan en la gestión de su propia seguridad y privacidad. »

Xavier Codó
CEO de ICAR



« Uno de los principales retos para las empresas es encontrar **el equilibrio entre experiencia de usuario y seguridad**.

Los usuarios quieren una experiencia rápida, cómoda y fácil, pero a la vez necesitan sentir que sus datos están seguros en todo momento. Aprovechar al máximo las nuevas soluciones tecnológicas será esencial para ganarse su confianza y retenerlos.

Pero la clave no es ya la tecnología en sí, sino el conocimiento de los nuevos hábitos y comportamientos del consumidor y la capacidad de utilizar la tecnología para aprovechar al máximo este conocimiento. Es decir, para personalizar las relaciones con el usuario y ofrecerle una experiencia por encima de sus expectativas. »

La clave está en personalizar las relaciones con el usuario y ofrecerle una experiencia por encima de sus expectativas.

Fernando Cabello-Astolfi

CEO de Aplazame



« Para Aplazame **la experiencia de usuario es esencial**. Una de nuestras obsesiones es que todas las interacciones de un comprador con nuestro proceso de solicitud de crédito sean lo más transparentes y gratas posibles. Estamos convencidos de que una buena experiencia determina que alguien vuelva o no a confiar en ti. Y en el caso de los e-commerce, esa confianza es un factor determinante para cerrar una venta o fidelizar a un cliente.

Además, Aplazame —como cualquier método de pago online— tiene el reto de ser extremadamente rápido, ágil y seguro. **Y aquí la tecnología juega un papel fundamental**, por ejemplo con soluciones que nos permiten automatizar la captura, reconocimiento y evaluación de la documentación que aportan nuestros clientes para darles respuesta inmediata a sus solicitudes de financiación. »

Una buena experiencia determina que alguien vuelva o no a confiar en ti.

5.

Normativa y regulación

Uno de los grandes retos a los que se enfrentan las empresas es cumplir con la normativa y la regulación actuales en tecnología.



Según algunos expertos, las empresas deberían contribuir a comunicar la dimensión real y las implicaciones de las nuevas tecnologías.

Pero, ¿Deben las empresas simplemente adaptarse a la normativa o bien contribuir a su evolución? Según algunos expertos, las empresas tienen que ir más allá, explicar y comunicar la dimensión real y las implicaciones de las nuevas tecnologías, con la finalidad de mejorar la comprensión del usuario.

Por ejemplo, con la tecnología actual las empresas pueden permitir el acceso a servicios financieros a segmentos de población underbanked o unbanked, es decir, con poco o ningún acceso a los servicios bancarios, un papel que va más allá de la regulación. En cualquier caso, la regulación no debería suponer un freno a la innovación.



ICAR
Qué nos ha enseñado el #MWC17 sobre el futuro de la identidad digital | 17 de marzo de 2017

La legislación que regule el ecosistema financiero digital debería ser internacional, para poder cubrir las operaciones y transacciones realizadas desde cualquier punto y hacia cualquier punto del planeta.

90% de personas

se preocupa por el tipo de información que se compila sobre ellos.

Americans' Attitudes About Privacy, Security and Surveillance. Pew Research Center 2015

60% de personas

cree que proteger su información financiera puede ser "tan complejo como aprender ingeniería aeroespacial".

Mastercard Safe and Security Survey 2015

54% de operadoras

ven el almacenaje, privacidad y protección de datos como la principal barrera legislativa para la innovación.

Global Fintech Report 2017. PwC

Josep Grau
CaixaBank Innovació



« Aunque las compañías utilicen los datos de usuario y puedan beneficiarse, hay ciertas líneas que nunca pueden ser traspasadas. Por ejemplo, **los datos tienen que ser siempre del usuario**, y este debe poder hacer realidad conceptos como el derecho al olvido, la portabilidad o modificación de tales datos. En un mundo tan cambiante y global como en el que vivimos las leyes tienen que ir adaptándose a nuevos contextos, y es en este contexto que nace la GDPR.

El objetivo del GDPR es proteger la privacidad de los datos de todos los ciudadanos de la UE.

Muchas empresas ya se han adaptado a tal directiva y están preparadas para su llegada, entre otras cosas porque la GDPR contempla sanciones ejemplares para aquellos incumplimientos de la normativa.

El Reglamento General de Protección de Datos de la UE (GDPR) sustituye a la Directiva 95/46 / CE relativa a la protección de datos, y fue diseñado para armonizar las leyes de privacidad de datos en toda Europa, proteger y empoderar a todos los ciudadanos de la UE.

Así, el objetivo del GDPR es proteger la privacidad de todos los ciudadanos de la UE de las violaciones de datos, en un mundo cada vez más centrado en los datos que es muy diferente de la época en que se estableció la directiva de 1995. Aunque los principios clave de la privacidad de los datos siguen siendo fieles a la directiva anterior, esta normativa comporta muchos cambios a las políticas reguladoras. »

Santiago Nadal
Socio Fundador de SNAbogados



« Con las nuevas tecnologías ha surgido un nuevo tipo de contratos que son doblemente novedosos. Por una parte regulan operaciones que ahora se hacen online y antes no existían; y por otra se "firman" online, a través de nuevas formas de contratación. Además, estos contratos suelen tener otros elementos innovadores: no se firman y se ejecutan de manera automática.

Se denominan smart contracts o contratos inteligentes. Hoy en día, se utilizan para operaciones en criptomoneda (crypto currency) como bitcoin, o para operaciones de financiación en masa (crowdfunding) de proyectos necesitados de inversión, o en sistemas informáticos de apuestas online.

Un smart contract es un programa informático que permite llegar a un acuerdo online entre varias partes y ejecutar dichos acuerdos registrados online. Son contratos automáticos que funcionan en base al principio if-then (si-entonces) de cualquier otro programa de ordenador. La persona A ordena al programa que, si la persona B hace algo, ocurra algo.

Cuando se dispara una condición pre-programada, el smart contract ejecuta una consecuencia, contenida en cláusula contractual: se ejecuta una obligación para la otra parte.

Los smart contracts dan una seguridad superior a la del contrato tradicional y reducen costos de transacción. Se produce una transferencia de valor digital, mediante un sistema que no requiere conocerse personalmente.

Estos contratos inteligentes pueden ser perfectamente válidos y suelen tener **un importante elemento internacional**, un elemento esencial en el ámbito de las transacciones digitales. Lo que será decisivo en estos contratos es determinar cuál es la ley aplicable, en caso de que surja el conflicto. »

Elaborado por:



www.icarvision.com

Colaboradores:















